WHITE PAPER

ServiceNow Security Best Practices Guide

Key considerations for securing Now Platform® instances

Release: Washington, DC

servicenow

Introduction

This document provides guidance on key considerations customers should address when securing their Now Platform instance under the ServiceNow Shared Security Model.

Please note: all information in this white paper is related to the ***standard Now Platform commercial environment****.*

For information related to other globally located ServiceNow in-country cloud offerings and how these offerings may differ, please contact your ServiceNow account representative.

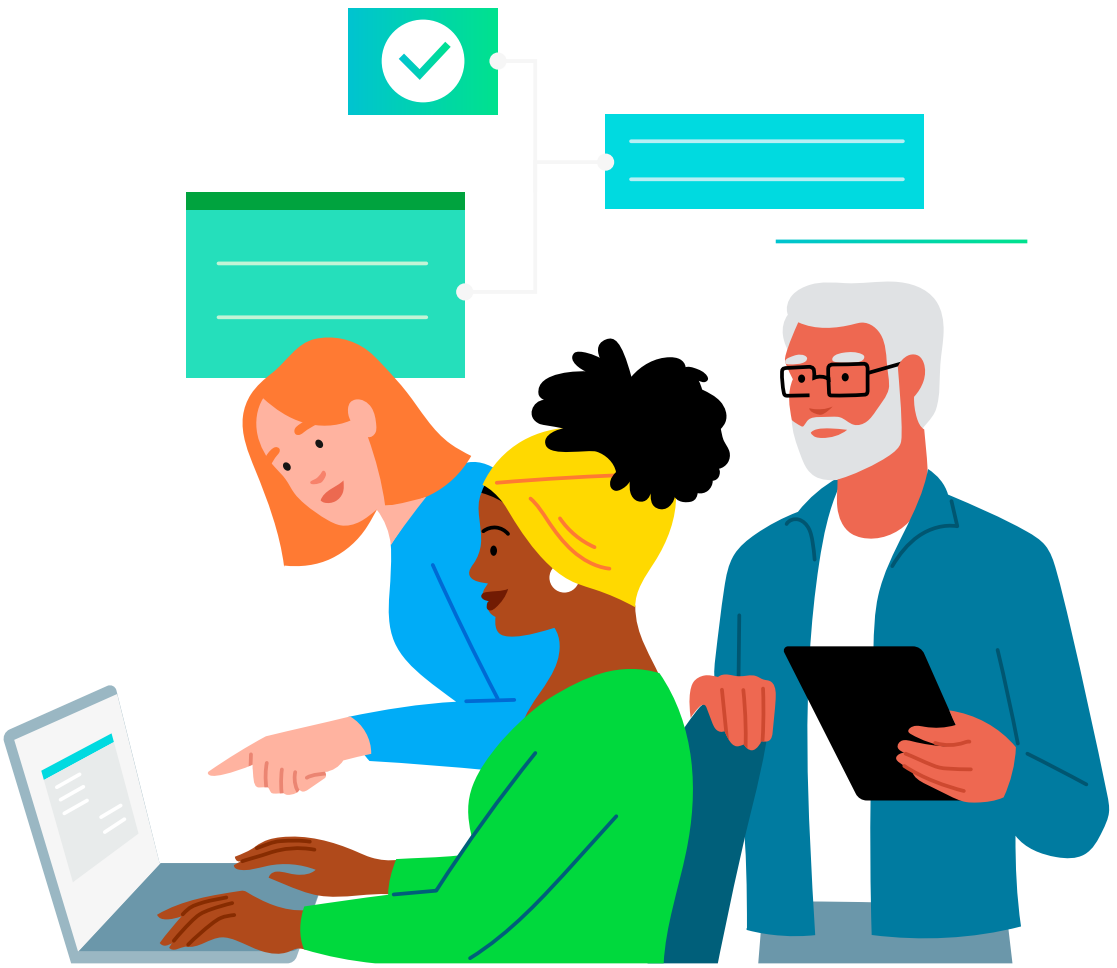


Table of contents

Introduction **2**
Security roles and responsibilities 4
Certifications and accreditations 5
Getting started: essential tools and guidance **5**
Security contact details 5
ServiceNow High Security Plugin (HSP) 5
ServiceNow Security Center (SSC) 6
Software updates 7
Email security 8
Logging and monitoring 9
MID Server security 11
Access control **12**
Authentication 12
Authorization 14
Encryption **16**
Column Level Encryption (CLE) 16
Full Disk Encryption (FDE) 17
Platform Encryption 17
Other important considerations **19**
Mobile application security 19
Secure Coding 19
Vulnerability assessment and penetration testing 20
Resources **21**

Security roles and responsibilities

Security is a partnership between the provider and customer, both with specific responsibilities.

ServiceNow provides its customers with extensive capabilities to configure their Now Platform instances to meet their own security policies and requirements.

The areas of responsibility are outlined in the table below. For more information about security responsibilities with respect to customer data, it is highly recommended to review the ServiceNow Shared Security Model.

> “Security is a partnership between the provider and customer, both with specific responsibilities.

Area of Responsibility	Responsibility		
	Customer	ServiceNow	Colocation (data center providers)
Secure configuration of instance	●		
Authentication and authorization	●		
Data management (classification and retention)	●		
Data encryption at rest	●		
Data encryption in transit	●	●	
Encryption key management	●	●	
Security logging and monitoring	●	●	
Secure SDLC processes	●	●	
Penetration testing	●	●	
Vulnerability management	●	●	
Privacy	●	●	
Compliance: regulatory and legal	●	●	●
Employee vetting or screening	●	●	●
Physical security/environment controls	●	●	●
Cloud infrastructure security management		●	
Infrastructure management		●	
Media disposal and destruction		●	
Backup and restore		●	
Business continuity and disaster recovery		●	

Certifications and accreditations

ServiceNow provides highly resilient and secure cloud-based services to customers all around the world. Ensuring that customer data is protected is always a top priority.

To demonstrate this commitment to customers, ServiceNow maintains many global and regional security and privacy certifications including the internationally recognized ISO 27001, ISO 27017, ISO 27018, and ISO 27701. A full list of security-related certifications are publicly available on the Compliance page of the ServiceNow Trust site.

In addition, ServiceNow provides transparency into its security program by providing prospects and customers access to certifications, attestations, standard operating procedures, and results of penetration tests and 3rd party audits through the CORE Compliance Portal.

Find out how to access the CORE Compliance Portal here.

Getting started: essential tools and guidance

Best Practice: All configuration changes should be tested on a non-production instance before being implemented on a production instance.

Security contact details

The ServiceNow Security Office (SSO) occasionally needs to relay security-related information directly to the appropriate information security contacts within an organization. The type of information could be informing the customer of security issues, security alerts, or details about important software updates, etc.

- Ensure that the security contact record within the customer account *(located in Now Support)* is always kept up-to-date, with details of at least two appropriate information security personnel.
- Security contacts should be authorized to act on the information they receive, because it may be critically important.
- It is recommended that a distribution list is also added to the security contact field.

Best Practice: Set a reminder to review the security contact details at least quarterly to ensure they are current and accurate. Including a distribution list is highly recommended.

ServiceNow High Security Plugin (HSP)

To help customers secure their instance easily and efficiently, ServiceNow provides the High Security Plugin. The HSP is a tool for enhancing security management and applying appropriate settings.

HSP is installed and enabled by default on all new instances. Older releases may require HSP to be explicitly activated.

The HSP Plugin enables High Security Settings, and the resulting actions include centralizing critical security settings, creating a distinct security administrator role, a default deny property, and others.

Default deny property: This property sets a default deny posture which prevents read, write, create, and delete for all tables unless explicit permission is given for a user or role in an ACL (Access Control List) rule.

Self-privilege elevation: Users with Security Admin privileges can elevate themselves when they need to perform operations requiring a higher privilege level. This action modifies ServiceNow system logs to be read-only and allows for controls to authorize access of properties.

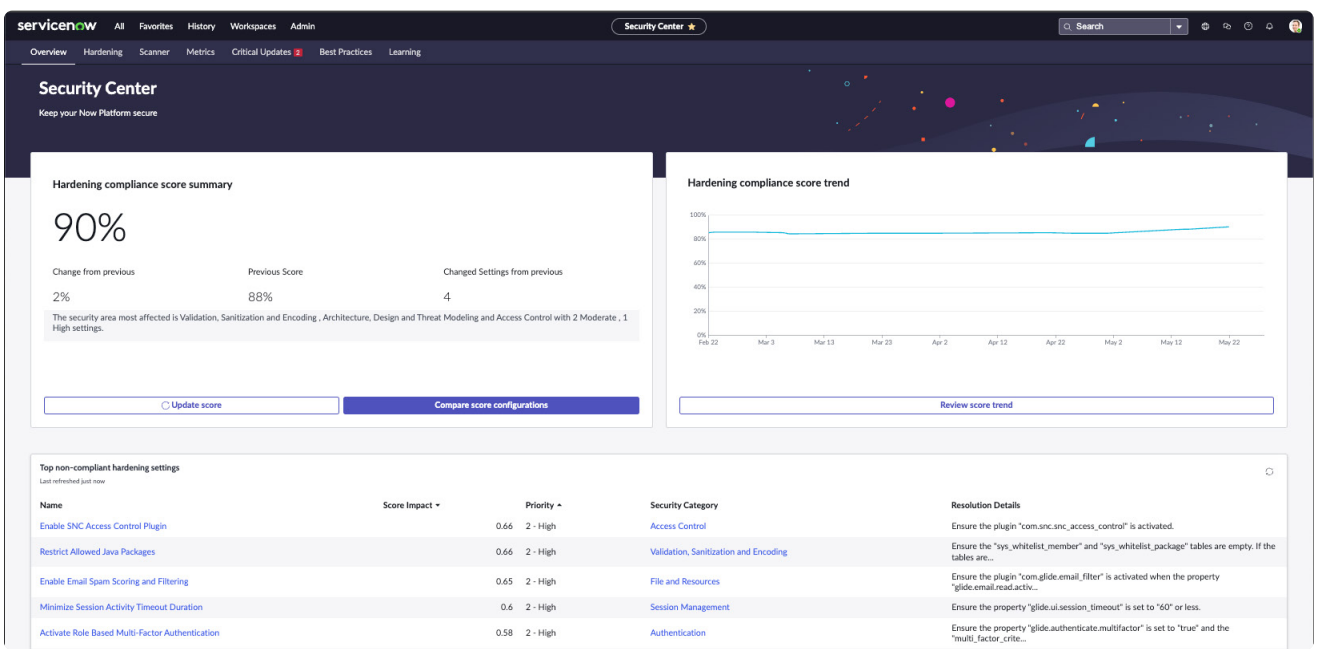
Best Practice: Ensure that the High Security Plugin is installed and activated, where possible, and enable the "default deny" property.

ServiceNow Security Center (SSC)

The ServiceNow Security Center is an application installed from the ServiceNow Store that has a set of tools designed to help customers easily improve the security and compliance of their Now Platform instances.

The SSC Security Hardening tool allows customers to view their compliance with the ServiceNow recommended settings as a percentage score, identify the top non-compliant hardening settings that improve compliance, and allows for easy changes of the settings to strengthen the security posture of their instance.

In addition, the SSC Security Metrics tool monitors over 60 different security KPIs, creates notification alerts to help identify potential security threats or insecure user behaviors.



Hardening settings

The Hardening settings describe ways to make a customer instance more secure and resistant to malicious intrusion. The Instance Security Hardening content also provides details about which settings and configurations must be applied *(mandatory)* and should be applied *(recommended)*, where possible.

- Some of the hardening settings require an understanding of the usage context, which is why those settings are not enabled by default.
- The ServiceNow Security Center (SSC) can greatly assist customers with assessing and working towards compliance with the recommended hardening settings.
- It is recommended to initiate ServiceNow Security Center updates in a sub-production instance to become familiar with any changes.

Best Practices:

- **At a minimum quarterly, consult the ServiceNow Security Center to assess and monitor the instance's overall security level.**
- **Enable the weekly digest notification for alerts about potential issues.**
- **Use the Hardening tile to research, test, and identify areas of noncompliance in a sub-production instance to assess impact to the environment.**

Software updates

As with any software product, a Now Platform instance requires maintenance and updates from time to time. This is achieved by applying the patches and upgrades made available through the ServiceNow Patching and Upgrades Program.

ServiceNow Patching Program

The ServiceNow Patching Program updates customer instances to required patch versions throughout the year. With this program, instances receive the latest security, performance, and functional fixes. Most importantly, patching remediates known security vulnerabilities and is an essential component of any patch management process.

More detailed information about the program is available to customers in the ServiceNow Patching Program FAQs.

Upgrades

Periodically upgrading the software version allows customers to benefit from enhanced functionality, performance, security, and usability. There are typically two major platform upgrades released every year. Upgrades can be installed at the customer's convenience, within the bounds of the ServiceNow End-of-Lif (EOL) policy.

- The Upgrade Center helps customers plan and manage their upgrades by previewing changes, monitoring the process, and viewing historical information.
- ServiceNow strongly advises customers to upgrade at least once per year.

End-of-Life (EOL) policy

To help ensure the highest levels of security, ServiceNow requires customers to keep up to date with platform releases, the ServiceNow EOL policy reflects this.

ServiceNow usually releases two major version updates per year and only supports the current version (N) and one prior release (N-1).

Older versions are considered "end-of-life" are no longer supported, and must be upgraded by a specified date to ensure the security of both the customer instance, and those of all other customers. After this date the customer instance will be automatically upgraded, if necessary.

Best Practice: Aim to install patches and platform updates as soon as possible to ensure the highest levels of security for both the customer's own instance and those of other customers. Conforming to the EOL policy also enables customers to maintain continuous support. Customers can use the Upgrade Center to help manage this process.

Email security

The Now Platform provides multiple capabilities for email security. These include controlling which inbound messages are accepted and from whom, encrypting the transmission of outbound messages, and scanning the contents of any attachments for malicious content. Customers can choose which of these capabilities to enable as appropriate to enforce their security policy.

Anti-malware and SPAM filtering

Malware scanning is performed by ServiceNow Antivirus Protection.

If a malicious email or attachment is detected, it is stored within an email quarantine area in a customer instance for inspection by their security personnel.

Additionally, all email inbound to the Now Platform is analyzed for malware and SPAM scoring and the results are reflected in x-headers added to the messages. Customers can use these as criteria for the Email Filters Plugin to act on, if desired.

Email domain restriction

Customers can control the domains and users their instance can send email to and receive from by using system address filters. These can be customized to meet customer requirements.

- An organization may control inbound email with anti-spam technology using Sender Policy Framework (SPF). If so, their email systems need to accept email originating from their Now Platform instance. This is best achieved by configuring them to dynamically query the ServiceNow SPF records.
- If SPF is not an option, another approach is to add the ServiceNow mail server IP addresses to the "allow" list. This does need to be monitored, as the addresses could be subject to change.

Automatic user account creation

This feature allows user accounts to be created dynamically by email, so it should be used with care. Only activate this feature if necessary for a specific use case.

Customers should ensure that they define a list of trusted domains from which accounts can be created. Customer admins can control how passwords are assigned to new accounts when they are created this way.

Email monitoring

Customers can monitor email and anti-malware activity in the ServiceNow Security Center (SSC). The SSC will highlight potential issues and provide guidance for any corrective actions that may need to be taken.

Email encryption

Now Platform instances have a built-in feature allowing send and receive of email using opportunistic TLS.

If a customer's email server accepts TLS, messages will be transferred over an encrypted session, using TLS *(TLS 1.2 as a minimum)*. This greatly enhances the privacy and integrity of messages as they traverse the internet.

ServiceNow also supports the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. S/MIME is an end-to-end encryption protocol for sending digitally signed and encrypted emails that support data confidentiality, authenticity, and integrity.

Customers using their own servers

Customers can use their own SMTP, POP3, or IMAP servers for more control over how mail is filtered, and received, before being ingested by a Now Platform instance.

Customers using their own email servers is considered an advanced email configuration, and can optionally use a third-party email infrastructure via OAuth 2.0 email authentication.

Best Practices:

- **Use the Now Platform email filters feature set to deal with suspect inbound messages, and limit accepted sender domains.**
- **Ensure automatic account creation is configured securely, or disabled if not needed. Ideally, customers should configure their email systems to accept mail from their instance by using Sender Policy Framework.**
- **If a customer already has a mature email security environment, they may consider using their own (or a third-party) infrastructure to send and receive instance-related email gaining the benefit of more precise perimeter email control.**

Logging and monitoring

A Now Platform instance performs detailed logging about many aspects of its operation.

These logs are stored within the instance itself, and benefit from the same level of security as other data in the instance. Application logs cannot be inspected by ServiceNow without a customer's permission.

Logs are a valuable source of security information that help highlight suspicious or malicious activity, so it is essential that they are adequately monitored. Customers can feed selected log activity to their SIEM *(or any syslog server)*, using the syslog probe.

The syslog probe is enabled via a Management, Instrumentation, and Discovery (MID) Server deployed in their network. Options are also available for direct customer SIEM integration which facilitate real-time logging as part of the Vault security bundle.

A customer's information security policy can provide guidance on which types of events are of interest and should generate alerts.

Here are some examples of notable activity:

- **Privilege escalation**
  Unexpected modifications made to privileged roles, such as Admin, ITIL_Admin, and any other roles with higher privileges that could indicate suspicious actions.
- **Failed logins**
  Unusual numbers or patterns of failed logins can reveal potential brute force attempts, or password spray attacks.
- **Admin users added**
  New admin account creation should always be checked for validity, in case of attempts at unauthorized privileged access.
- **SNC Logins**
  Customers can monitor any ServiceNow access to their instance, and the actions performed.
- **Quarantined files**
  The ServiceNow Antivirus Protection detects potentially malicious files uploaded to a customer instance. These files should be monitored for sources and frequency.
- **Impersonations**
  Monitoring for elevated account impersonation helps highlight any potentially dangerous, unnecessary, or unauthorized privileged access.

The ServiceNow Security Center (SSC) can also provide valuable insights.

Event logs

Event logs reveal much about system activity, including login events *(successful or otherwise)* and privilege escalation.

System logs

System logs contain extensive information about general activity, including configuration changes, system errors, workflows, and inbound/outbound data connections.

Audit logs

The Event and System logs can also be used to provide an audit trail of any activity by ServiceNow personnel.

Transaction logs

Transaction logs record all web-browser related activity for an instance and can provide details of every request made. These logs can be very useful for identifying unusual or malicious activity.

Table auditing and record history

Customers can enable auditing for database tables making record history perpetual and allowing customers to track and view details of any changes made to the data since creation. By default, only the incident, problem, and change tables are tracked. For other tables, auditing needs to be enabled manually.

Import logs

Customers can view detailed information related to data import activity on their instance by checking the import logs. This includes information about source, status, time, etc.

Outbound web services logs

Outbound web services logs show REST and SOAP request activity and can help customers keep track of the volume and destination of connections to external services.

API Analytics

Customers can track and analyze inbound REST and SOAP activity with API Analytics. These analytics help the customer to understand which APIs are being used, by whom, and to what degree.

Log archival

Customers may wish to transfer log data from their instance to their own environment for archival *(beyond the default log rotation period)*. The log rotation period varies depending on the log type.

Browser SQL error Messages

Improper web queries can result in error messages from the database engine, presented in the web browser. Though these queries can be useful to end users and developers, they can also be used by would-be attackers to glean information about the underlying system, or to help guide their attempts to access the system.

Customers can add a system property to disable SQL error messages.

> “Logs are a valuable source of security information that help highlight suspicious or malicious activity, so it is essential that they are adequately monitored.
>
> The ServiceNow Security Center can also provide valuable insights.

Best Practices:

- **Enable table auditing for important or sensitive data.**
- **Monitor important logs to help identify any suspicious or malicious activity.**
- **Use the syslog probe to send logs to a customer's SIEM which will allow activity monitoring and help identify security events.**
- **Transfer log data from the customer instance for archival and reference.**
- **Disable browser SQL error messages.**

MID Server security

The ServiceNow MID Server is a Java application that runs as a service on one or more servers on a customer network, which is designated for that role.

The MID Server acts as a conduit to the customer's infrastructure *(and services)* that need to communicate directly with the Now Platform instance. These services might be internal or external to the customer network and can include directory services, logging, or infrastructure management systems.

Physical security

The MID Server is a critical piece of infrastructure and may contain sensitive information. As with any other important infrastructure, it should be located within a secured environment *(e.g., a data center or server room)* with good physical security and controlled access.

Server platform

The MID Server Java application runs on supported Windows or Linux Servers with a Java Runtime Environment. Installation packages are digitally signed for security.

The server operating system and runtime environment should be deployed, secured, and hardened in line with the customer's existing internal IT security policy and operating procedures.

Network connectivity

Communication from the MID Server to a customer instance is only ever outbound; on their local network it is only to systems that they determine.

All outbound connections are via HTTPS on port 443. Customers can explicitly disable SSL to ensure that only TLS *(TLS 1.2 as a minimum)* is used.

- MID Servers must be able to connect to https://install.service-now.com for automatic updates and can use a web proxy for outbound connections. MID Servers can upgrade directly from the instance itself.
- On the internal network, the MID Server uses a variety of ports and protocols according to the resources it is connecting to, e.g., SSH, WMI, SNMP, etc.
- The customer admin should ensure that they exclude *(or disable)* the MID Server during any internal vulnerability scanning, to avoid creating unnecessary traffic to their instance.

Other MID Server considerations

There are extensive options for protecting MID Server data with encryption.

- Customers can encrypt credentials stored within configuration files, supplying TLS certificates for mutual network authentication, enabling certificate validation, code signing, and requiring authentication for web services, API, and SOAP connections.
- Customers should store credentials the MID Server uses for service connections in a secure external storage system for additional protection.
- ServiceNow recommends that customers enable the MID Server command audit log, which records the commands run for the Discovery application. Customers should also regularly review the log to check for anomalies or errors.
- The MID Server supports Microsoft Just Enough Administration (JEA) for basic discovery. This uses role-based administration through PowerShell Remoting and removes the need for discovery accounts to have full admin privileges.
- Client-Side Secrets Management capability, included in ServiceNow Vault, allows customers to secure secrets at the MID Server, so the private key is not housed in the Now Platform instance.

Best Practices:

- **Ensure the MID Server is in a physically secure, controlled location and that the operating environment has been secured and hardened.**
- **Enable only the minimum connectivity necessary between the MID Server and the internal and external network, allowing for required services and infrastructure.**
- **Disable the use of SSLv3.**
- **For additional security, customers can encrypt stored credentials, enforce certificate validation, and supply TLS certificates.**
- **Protect service credentials in a secure storage system.**

Access control

Every user must have an associated unique user account defined within the Now Platform instance, and their identity must be established before access is granted. The most important methods for controlling access to a customer's instance are user **authentication** to verify identity, and **authorization** to control access levels and permissions.

Outbound IP access controls are configured using the IP Address Access Control feature in the Now Platform. Additionally, ServiceNow supports the System for Cross-domain Identity Management (SCIM) protocol, which allows customers to synchronize user and group data from external identity providers.

Authentication

Account and password control

Now Platform instances come with certain built-in accounts such as "admin," "ITIL," and "employee" which are provisioned with default passwords unique to the instance. Default passwords should be changed as soon as possible.

- Customers have full control over the password policies enforced for access to their instance. For native or local accounts, customers can specify length, complexity, expiration, uniqueness, lockout, etc. *(this can be* set in the GUI*)*. To maximize security, encourage the adoption of long passphrases and aim to eliminate the use of simple, "common" passwords. Customers can of course retain their existing policies for any external authentication services they have integrated, such as LDAP, SAML, etc.
- There are some security-related adjustments to the login page to consider. "Remember Me" is a feature for caching user login page credentials in a browser. This feature can present security issues if users access their instance from an unsecure endpoint, e.g., from a shared computer. The Instance Hardening Guide recommends disabling this feature.
- Remove credentials from the Welcome page and password-less authentication *(logging in to the Now Platform with blank passwords).*
- Configuring account lockout after a number of failed logins within a certain time frame can help guard against brute force authentication attacks.
- ServiceNow provides further guidance on enhancing authentication security in the Defending Your Now Platform instance Against Password Spray Attacks *(requires a Now Support account)* knowledge base article.
- Activating the System for Cross-Domain Identity Management (SCIM) plugin allows customers to easily provision and manage user identities, group membership and other properties from sources external to their instance, using an industry-standard protocol. These typically include cloud-based services like Active Directory, Amazon Web Services, Okta and others. The ServiceNow SCIM features frees customers from having to create and manage multiple customized SOAP APIs.

Authentication mechanisms

The Now Platform offers a selection of authentication mechanisms.

Basic or native authentication uses local accounts defined within the instance, while SAML 2.0, LDAP, OAuth2.0, and certificate-based authentication enable integration with external services.

SAML 2.0 is often preferred as an authentication method as it is very secure and widely used. Most customers will already have some form of SAML Identity Provider (IdP) such as ADFS, Ping, or others.

- Multi-provider Single Sign On (SSO) makes it possible to combine SSO with other authentication methods, including Open ID Connect (OIDC). OIDC allows users to authenticate using third-party credentials, such as credentials from Google, Azure, Okta or others.
- For high-security environments, customers can use Personal Identity Verification (PIV) card or Common Access Card (CAC) authentication as an extension of certificate-based authentication, where certificates are stored on a smartcard.
- Customers can help prevent unauthorized access to their instance, unrelated to their organization, by setting an Inbound IP access restriction. For this access restriction ServiceNow recommends using Adaptive Auth, typically only allowing external addresses from the customer's gateway or web proxy. Anyone trying to access the instance from an unauthorized range will be denied. If using this approach, consider where all users access the instance from, e.g., remote users. Customers can control outbound as well as inbound access by IP address.
- Adaptive Authentication allows a combination of criteria including IP address, role, and group membership to be used to create granular access control policies. These can be applied to Web Services/APIs as well as to normal user access.

Access via Account Recovery (ACR)

If a customer's instance has issues with, or failure of, their external authentication system, customer administrators can configure Account Recovery (ACR) to perform recovery activities such as addressing SSO misconfiguration, or expired certificates.

> *Note: Enabling ACR disables the local interactive logins (username or password based) when SSO is enabled on an instance.*

ACR provides the following capabilities:

- The ability to bypass Single Sign-on (SSO) login, to address issues with SSO configuration as an administrator.
- Login using SSO to perform tasks with an administrator account, configured as an account recovery.
- ACR flows which enable customer administrators to use self-service capabilities to address account recovery when there's a need for recovery. For example, when there is a SSO misconfiguration, or expired certificates.
- Reduce unauthorized access to the instance and provide a strong foundation to use ACR outside SSO use cases.

To use Account Recovery, customer admins must register at least one admin account as an Account Recovery (ACR) user. Single sign-on can't be activated on an instance until there is at least one account configured.

For details on this process, see configure an account recovery user from the Account Recovery Properties page.

Multi-Factor Authentication

Third-party Multi-Factor Authentication (MFA) as well as time limited authentication can be integrated with a customer's existing SAML IdP to provide additional login security.

MFA provides a high level of security because authentication requires something the user knows *(the password)* as well as something they own *(such as a One-time Password [OTP] produced by a MFA token or mobile phone)*, or a physical attribute *(such as a fingerprint or facial recognition).*

Users logging into a system with MFA enabled must provide this additional credential along with their username and password.

- The Web Authentication integration, allowing physical keys and biometric data such as fingerprints or facial recognition to be used with MFA.
- The Now Platform supports direct MFA integration with local accounts, LDAP, and for SSO with SAML, OIDC, or Digest. The expansion of this feature allows conditional, rigorous authentication for e.g., remote users. Adaptive Authentication is a prerequisite for SSO with MFA.
- MFA can be enabled for specified users and specified roles, and configured for ease of use, e.g., to exempt recognized devices for a number of hours. ServiceNow recommends that customers enable MFA by default for all Admin users. MFA is supported for SSO integration, and ServiceNow offers built in MFA options, as well as email and SMS One-time Password (OTP).
- Customers can view Metrics for MFA use in the ServiceNow Security Center.
- Customers can use Adaptive Authentication to enforce contextual authentication controls to the right users at the right time. This included Step-Up or Step-Down MFA polices.

Monitoring

ServiceNow strongly recommends that customers monitor security events in the ServiceNow Security Center for unusual activity such as high numbers of failed logins, especially within short time frames. Now Platform instances can create incident tickets, or trigger, workflows *(e.g., notify a customer's security response team automatically when user-defined criteria and thresholds are met)*.

- Use the Session Management tile in the ServiceNow Security Center to view detailed information about all user sessions and lock out any that could present a risk.
- Optionally, customers can use a data filter to narrow the scope of their data filtration rule to apply only to specific records on a table. The data filter also allows monitoring of high privileged users and notifications when new admins are created.

Authorization

Once a user has successfully authenticated, access to parts of the instance interface, functions, and the data within it are controlled with Access Control Lists (ACLs) and Role-Based Access Control (RBAC).

ACLs use the account ID and associated groups to determine what access should be granted to an object, e.g., read, write, delete, create, etc.

- RBAC rules are ACLs assigned to roles defined within the instance. These might cater to different types of users or various job roles. User accounts and groups are assigned to roles, and permissions are applied to those roles.
- To provide an extra level of protection, customers may want to limit concurrent sessions for the same account or role.
- If the High-Security Plugin *(see page 5)* is enabled, customers can set a default deny property, which prevents read, write, create, and delete for all tables, unless explicit permission is given for a user or role in an ACL rule.
- All new instances have the Security Jump Start – ACL Rules plugin installed, to provide a base level of access security for key system tables.

File attachments

Customers can place access controls on file attachments.

Uploads can be restricted by role, file extension, MIME type, or size, to help prevent potentially malicious files being stored and subsequently delivered from their instance.

Customers can also control which file types can be downloaded, including by MIME type, and prevent image access by unauthenticated users.

- The ServiceNow Antivirus Protection plugin is installed and activated by default. This performs anti-virus (AV) scanning on all attachments.
- Attachments can be encrypted. See the Encryption section in this document for more details.

Access by ServiceNow employees

Generally, ServiceNow personnel cannot access a customer instance without their authorization, except for Customer Support employees assigned to an open case for that customer. Any such access is strictly controlled and monitored, and customers can identify this activity at any time by tracking the occurrence of the identifier name@snc in the instance event logs. This is also tracked in the instance's Security Center widget.

Customers may choose to activate the ServiceNow Access Control plugin that enables customers to control which ServiceNow customer service and support employees can access their instance, and when. Once activated, ServiceNow personnel must explicitly request access from the customer on an ad-hoc, and temporary, basis.

There is more detail about ServiceNow access in the Securing the Now Platform white paper, including controls such as the ServiceNow Access Control plugin (SNAC).

Auditing access permissions

Customers can check which users have access to which tables, and to what degree, using the Contextual Security Auditor plugin. This plugin is an interactive tool which evaluates table access permissions and displays them in an easy-to-understand format and can be installed by Customer Support, on request.

Customers can also use another ServiceNow tool to audit access permissions, called Access Analyzer. Access Analyzer allows analyzation of the access control rules for a specific table or field, and allows customer admins to see which roles are required to perform read, write, create, or delete operations on that table or field.

Instance identification

The way customers name and brand their instance can help with security. Customers may wish to avoid choosing a name for their instance that obviously associates it with their organization, e.g., acmeinstance or mycompanyprod.

- Customers can rename an instance if necessary *(link requires a Now Support account)*.
- Customers should also carefully consider how they use branding and logos on the login page.

Best Practices:

- **Change the default login credentials. If possible, use SAML authentication, and integrate with MFA.**
- **Enforce the use of strong passphrases and restrict access to a customer instance from unknown IP addresses.**
- **Review the ServiceNow guidance on password spray attacks and disable password-less authentication.**
- **Remove the "Remember Me" checkbox and default credentials from the login page.**
- **Monitor the logs for high numbers of login failures and create alerts accordingly.**
- **If the instance has been used from older releases and HSP is not activated, enable the High Security Plugin to activate the default deny property.**
- **Add granular control with RBAC.**
- **Use encryption modules with RBAC to further enhance data access control.**
- **Consider limiting file attachments, uploads and downloads.**
- **Consider using the ServiceNow Access Control plugin to control specified users at ServiceNow that have access to the Now Platform instance.**

Encryption

The Now Platform can encrypt data to maintain its confidentiality and integrity. While in transit, data is secured with TLS *(TLS 1.2 as a minimum)*. While at rest, data fields can be configured to be encrypted within the database and/or customers can elect to subscribe to functionality to encrypt the data volume transparently on the backend. The physical disks on which the instance runs can be encrypted *(in their entirety)* to guard data in case of their loss or theft.

For data stored in a Now Platform instance, customers can use different types of encryption simultaneously. Customers should select these according to their use case and the risks that they wish to mitigate. For example, a customer might choose to transparently encrypt their data at rest, data fields can be configured to be encrypted at the application layer, cloud encryption on the entire data volume, or leverage hardware Full Disk Encryption (FDE) — which also requires a dedicated environment to protect against drive or server theft.

Information transferred between a customer's Now Platform instance and any external services customers have integrated with *(e.g., authentication, file transfers, or web services extensions)* can also be encrypted. This is also true of traffic to and from the MID Server.

Column Level Encryption (CLE)

Data stored within a Now Platform instance, including attachments, can be protected with Column-Level Encryption (CLE) using AES128, or AES256. This allows encryption of specified database columns and attachments through use of cryptographic modules.

- These cryptographic modules provide role-based access control and enable customers to decide what columns are encrypted, what algorithm is used, which encryption key is utilized, and what roles/processes/services will have what access type to the data.
- The key itself is stored within the instance and is protected via the Now Platform NIST 800-57 compliant Key Management Framework (KMF).
- The encryption key is also protected by a wrapping mechanism, through several other keys stored within the customer instance and the ServiceNow Key Management System (KMS).
- The Password2 field type in ServiceNow is an out-of-the-box feature specifically designed for the secure storage of sensitive data. When data is entered into this field, it's encrypted using a dedicated cryptographic module. This encrypted field is particularly useful in scenarios such as system integrations where authentication credentials, like API keys are stored, or in custom ServiceNow applications where sensitive information needs to be safeguarded.

Platform Encryption

Platform Encryption combines Column Level Encryption Enterprise with the new Cloud Encryption capabilities.

Column Level Encryption Enterprise (CLEE)

Column Level Encryption Enterprise is available as a subscription as part of the Platform Encryption bundle. This encryption option is similar to the Column-Level Encryption (CLE), but with multiple additional capabilities, such as application-level field encryption, attachment encryption, and API support.

API support enables automated processes and workflows to function on encrypted data and enhanced key management with the option of customer-supplied keys, Bring Your Own Key (BYOK).

CLEE employs Cryptographic Modules in which an encryption key, scheme, and policy are combined to allow flexible and granular cryptography for instance data.

Cloud Encryption (CE)

Cloud Encryption (CE) is an additional cost option available with the Platform Encryption bundle. Cloud Encryption enables encryption of the database storage volume at rest and ensures compatibility with database technology enhancements that ServiceNow may introduce in the future.

Cloud encryption provides protection in the unlikely event of physical disk loss or theft.

Cloud encryption also uses the KMF, and therefore benefits from NIST 800-57 compliant key lifecycle management, including segregation of duties, rotation of ServiceNow-managed keys, and the option of Customer Managed Keys (CMK).

CE Withdraw and Resupply capability allows customers to withdraw their CMK and leverage Quorum control for approval operations to trigger a shutdown of their instance, until a restore operation is performed to resupply the withdrawn key.

If the withdrawn customer managed key isn't restored within the time frame for which ServiceNow retains backups, the instance database backups will no longer be accessible. Backup data lost in this way isn't recoverable.

For more details please see the Backup and Restoration SOP *(requires access to the ServiceNow CORE Compliance Portal. Find out how to request access here).*

Key Management Framework (KMF)

Now Platform Key Management Framework is the foundation of Column Level Encryption Enterprise (CLEE) and Cloud Encryption (CE).

KMF utilizes encryption for key storage which is FIPS 140-2 validated, Bring Your Own Key (BYOK), improved key management throughout the NIST 800-57 based key lifecycle, and many other benefits, including the ability to transfer keys securely between instances.

Tamper detection is available with the quorum control settings associated with withdrawal capabilities. This protection enables customers to be notified if any settings associated with the defined quorum control process have been modified.

Full Disk Encryption (FDE)

Full Disk Encryption is an additional cost option which encrypts off the physical drives used for customer instance database storage.

FDE requires customers to purchase a dedicated environment for their instances. This capability encrypts customer data in the instance when the system is offline and therefore provides protection in the unlikely event of physical disk loss or theft.

Integration traffic

Single sign-on (SSO):
With SSO, authentication can be performed using SAML integrations to the customer IdP using TLS. Secure Lightweight Directory Access Protocol (LDAP) and OAuth are also available for authentication and user object synchronization.

File transfers:
Files can be made outbound from a customer's instance with SFTP, FTPS, or SCP. Outbound clear text protocols such as FTP and HTTP are also supported, but not recommended.

Inbound transfers such as web uploads are conducted exclusively over HTTPS. In each case, TLS is supported. Email attachments are discussed in the section on email security.

Inbound and outbound:
Web-based connections to external REST/SOAP services are over HTTPS using TLS, and can use certificate-based mutual authentication. In addition, inbound REST APIs can be protected with adaptive authentication access policies, and SOAP requests can be digitally signed.

Outbound JDBC queries:
Outbound JDBC *(Java Database Connectivity)* queries can be made from a customer instance. This traffic is not encrypted but can be securely proxied via the MID Server.

Best Practices:

- **Configure web browsers to use only TLS 1.2, or higher, when connecting to their instance. This can be done on the browser itself, or enforced by the instance's web proxy (or other gateway).**
- **Encrypt data at rest within the instance using the method that best suits the customer's encryption needs. Traffic to a customer's integration provider(s) should be configured to use TLS wherever possible, with REST/SOAP connections making use of certificate-based authentication.**

Other important considerations

Mobile application security

To enable the use of an instance from a mobile device, customers can take advantage of native ServiceNow mobile applications for iOS and Android.

The ServiceNow mobile applications utilize OAuth 2.0 and benefit from the same robust authentication mechanisms of the Now Platform. These mechanisms can be augmented with MFA and AppAuth. Once authenticated, mobile users are subject to the same access controls as other Now Platform users.

Customers should use the Zero Trust Access — Session Access policy within the Adaptive Authentication policy to reduce the roles or privileges of a particular session for mobile users.

Mobile application security controls

Mobile-specific security controls are available and provide additional security for devices. These controls include restricting clipboard operations, requiring a PIN for access, disabling attachments, and obscuring the app screen when in the background.

Customers can enable re-authentication to re-validate user credentials as a requirement before performing certain actions within the app.

Mobile data security

All mobile data in transit is protected with TLS *(TLS 1.2 as a minimum)*, and application preference information is encrypted with AES256.

By default, only application preferences are stored locally. No record data is stored on the mobile device, though this option can be enabled by a customer admin it is not recommended. The record data is encrypted in storage.

Mobile application distribution

The mobile applications can be distributed with common Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) platforms.

Customers can use Mobile Application Management (MAM) to control, secure, and enforce policies for ServiceNow mobile apps. These tools provide a central point of control for securing customer data on mobile apps, even in scenarios where they are not the owner of the mobile device.

ServiceNow only supports Microsoft Intune and BlackBerry SDKs.

Best Practices:

- **Employ MFA along with a preferred authentication mechanism.**
- **Use the built-in controls for application access, clipboard, screenshots, etc.**
- **Avoid storing record data on the mobile device.**
- **Use an EMM or a MAM to ensure secure management of mobile devices and applications.**
- **Use the Zero Trust Access — Session Access policy within the Adaptive Authentication policy to reduce the roles or privileges of a particular session for mobile users.**

Secure Coding

Development of code, or applications, on a customer instance should follow good security practices. The Secure Coding Guide *(requires a Now Support account)* covers many topics in this area and gives recommendations on aspects such as input/output sanitization, session management, secure access and more.

Best Practice: Refer ServiceNow developers to the Secure Coding Guide to ensure that they follow the practices outlined.

Vulnerability assessment and penetration testing

Vulnerability assessment and penetration testing are vital for confirming the security of an instance and to identify and address any potential weaknesses. For this reason ServiceNow has developed a sophisticated vulnerability testing and remediation program to ensure the highest levels of security for customers.

Customers can also conduct their own application penetration testing to learn more about their instance's external security posture.

The ServiceNow testing program

ServiceNow uses a multi-layered testing program and SDLC for developing products. ServiceNow follows recognized industry best practice from organizations such as OWASP and NIST, among others. Throughout the development cycle, ServiceNow regularly tests against the most common web application threats, such as those specified in the OWASP top-ten, e.g., input validation, cross site scripting (XSS), and session management.

- The ServiceNow product security team regularly scans test instances of supported releases with a commercial web application scanner which has been configured and tuned specifically for the Now Platform.
  - Scans are modified as necessary to cover new features or platform changes.
  - Any validated findings feed into the development remediation process so that identified vulnerabilities are addressed prior to release.
  - The ServiceNow Vulnerability Management SOP describes this process *(requires access to the ServiceNow CORE Compliance Portal)*. Learn how to access CORE here.
- When checked into the main ServiceNow branch, code is statically tested for vulnerabilities. ServiceNow also performs internal, manual testing of any new patches and hot fixes developed through the lifecycle of a release family. In both cases, any detected issues enter the remediation process to be addressed, where necessary.
- Cloud infrastructure is internally and externally scanned for vulnerabilities *(at a minimum monthly)* using a third-party enterprise vulnerability scanner. Internal scanning is performed on an authenticated basis to ensure maximum coverage.
- An independent third party performs application penetration testing on all major releases, before making them available to customers.
  - Based on several factors, including overall risk and possible impact, validated findings are sent for remediation. Customers can request a summary of the results from these tests.
- ServiceNow rotates testing through several qualified providers in order to deliberately expose the platform to different teams, processes, and techniques. This maximizes the possibility of gaining actionable results during this stage of the overall process.
- Customers should review the most recent ServiceNow published penetration test reports on the CORE Compliance Portal. Find out how to access CORE here.

Customer testing

ServiceNow customers can perform a penetration test against a sub-production instance by following the Customer penetration testing policy *(requires a Now Support account)*. Any security testing outside of this process is not permitted.

At the conclusion of the authorized testing period, all findings that impact the platform must be reported to ServiceNow via the Security Findings application in Now Support. The process for submitting findings is detailed there.

- The target instance must be a non-production instance, running a supported update and hotfix combination.
- Customers must report their findings to ServiceNow within 30 days.

Best Practices:

- **Review the most recent ServiceNow published penetration test reports on the CORE Compliance Portal. Find out how to access CORE here.**
- **If a customer would like to carry out their own annual application penetration test, they must ensure that they have first installed the latest updates, hardened the instance, and fulfilled the prerequisite conditions described above.**
  - **After these steps are completed customers can schedule a test in the Now Support Portal. ServiceNow will respond to findings in accordance with the process described in the Customer Penetration Testing Policy** *(requires a Now Support account)*.

Resources

- ServiceNow Product Documentation
- Customer Success Center
- Securing the Now Platform white paper
- Cloud Security, Trust, and Compliance Center
- Instance Security Hardening Settings
- Defending your Instance against Password Spray Attacks
  (requires a Now Support Account)
- ServiceNow CORE Compliance Portal Directory
  (requires access to the ServiceNow CORE Compliance Portal, find out how to access here)

> Maintaining security is an ongoing process, it is always important to monitor activity, keep abreast of new developments, implement relevant changes, and verify the results at regular intervals.

servicenow